14

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/695,008	10/28/2003	Steve W. Rodgers	15128US02	4253

23446 7590 05/14/2007
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/695,008	**Applicant(s)** RODGERS ET AL.	
	Examiner Daniel L. Hoang	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

RESPONSE TO ARGUMENTS

Applicant's arguments filed 3/7/07 have been fully considered but they are not persuasive.

In response to applicant's arguments regarding the enablement and indefiniteness of claim 2, examiner respectfully withdraws the previous office action's 112 rejections of this claim. The indefiniteness rejections of claims 17 and 34 are also respectfully withdrawn as a result of applicant's arguments.

In response to applicant's arguments pertaining to the objections of claims 7, 10, and 21, examiner asserts that said arguments are not successful in overcoming the previous office action's objections.

As per claim 7, the parent claim cites that the decryptor is adapted to fixedly bit shuffle the bit-rolled data. It is clear to examiner that, in order for the decryptor to fixedly bit shuffle the bit-rolled data, the decryptor must comprise a fixed bit shuffler. Claim 7 cites that the decryptor comprises a fixed bit shuffler. Unless applicant intends that the parent claim fixedly bit shuffles the bit-rolled data using some other means outside of a fixed bit shuffler, the dependent claim is not further limiting.

As per claim 10, the parent claim cites the decryptor being adapted to add a first key to the bit-shuffled data. Applicant's specification explains that step is performed by an adder which is understood by examiner to be a component or module within the decryptor. Since the parent claim cites the ability of the decryptor to add, it is clear that the adder is already claimed in claim 1. Therefore, dependent claim 10, which claims the decryptor comprises one or more two-bit adders, does not further limit the parent claim.

As per claim 22, the parent claim cites the decryptor decrypts encrypted data. The parent claim also cites that the encrypted data is stored in the memory. In order for the decryptor to decrypt encrypted data, it is clear that the decryptor would have to receive it from the memory.

Therefore, claim 22, which cites that the decryptor is adapted to receive encrypted data from the memory, is not further limiting on the parent claim.

In response to applicant's arguments regarding anticipation rejection based on Richard:

Applicant argues:

Richard does not teach variably bit rolling, but rather generates a non-linear pseudo-random sequence. Examiner respectfully disagrees. Examiner interprets the combination of the non-linear pseudo-random bit sequence with clear text data is equivalent to bit rolling. Therefore, the rejections present in the previous office action are maintained.

In response to applicant's arguments regarding anticipation rejection based on Luyster:

Applicant argues:

As per claims 20 and 25, applicant argues that Luyster does not decrypt in a single cycle, but rather in a plurality of rounds. Examiner asserts that this argument is insufficient to overcome the rejection. Applicant's claimed invention teaches that the decryptor decrypts a word of the encrypted data in a single cycle but does not specifically claim that the entire data is decrypted within a single cycle. It is possible to interpret the claimed "data" to comprise of more than one word and would also be further possible to interpret that the existence of more than one word would lead to more decryption cycles occurring. Applicant's specification also teaches that data can be comprised of roll regions and that bit rolling may refer to an ability to rotate bits within a particular roll region within a data set. For these reasons, the rejections present in the previous office action are maintained.

As per claims 19 and 24, applicant argues that Luyster does not teach the processor comprising a decryptor that decrypts encrypted data *without adding enough gate delays to exceed a clock cycle budget of the processor.* Rather, applicant claims that Luyster describes an encryption process that is iterative and requires a plurality of rounds. Based on the reasons above pertaining to claims 20 and 25, the rejections in the previous office action are maintained.

As per claims 1-23, 26-29, 30-37, applicant has amended the claims to further clarify that the bit rolling of the encrypted data is based on at least an address. Applicant argues that this new addition to the claim is not taught by Luyster. Examiner respectfully disagrees. Examiner believes that this was already implied in the previously submitted claims and that Luyster already teaches this. Luyster teaches the use of registers to bit roll data. Registers are the data locations in a microprocessor. It is clear that bit rolling using registers are based on at least an address or location. Thus the newly added amendment to the claims is insufficient to overcome the rejections present in the previous office action and they are maintained.

CLAIM OBJECTIONS

1. Claim 7 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim cites the limitation "the decryptor comprises a fixed bit shuffler". The parent claim already teaches that the decryptor is adapted to "fixedly bit shuffle the bit-rolled data.

2. Claim 10 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim cites the limitation "the decryptor comprises one or more two-bit adders." The parent claims teaches that the decryptor is adapted to add a first key to the bit-shuffled data. As is consistent with the applicant's specification, examiner fails to see claim 10 as further limiting claim 1.

3. Claim 21 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim recites the limitation "the decryptor is adapted to received encrypted data from the memory." The parent claim recites encrypted data stored in a memory and that the processor is coupled to the memory and that the processor comprises a decryptor that decrypts encrypted data. It is interpreted by

the examiner through the claim language of the parent claim that the decryptor is adapted to receive encrypted data from the memory.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2 are rejected under 35 U.S.C. 102(b) as being anticipated by Richard et al., US Patent No. 4,004,089, hereinafter Richard.

As per claim 1, Richard teaches:

A system for protecting data, comprising:

a memory in which encrypted data is stored; and

> *[see col. 3, lines 48-52] "A credit card read and write module 30 can be used to read the magnetic stripe of a credit card to provide an enciphered text data signal to the terminal central processing unit (CPU) 10."*

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data,

> *[see col. 3, lines 58-61] "The CPU 10 directs the enciphered text to the decrypting section, terminal 100, of the programmable cryptic device 20 for decoding. The decoded data is designated clear text."*

the decryptor being adapted to:

variably bit roll the encrypted data,

> *[see col. 1, lines 61-65] "the bit outputs from a plurality of linear shift registers are combined in a non-linear sequence generator to provide a bit substitution signal which signal is a long, non-linear pseudo-random sequence bit signal."*

to fixedly bit shuffle the bit-rolled data,

> *[see col. 2, lines 2-5] "A bit shuffler then shuffles the position of the bits in the partially encoded signal so as to perform the bit transposition process, and to provide the completely encoded signal."*

to add a first key to the bit-shuffled data and

> *[see col. 1, lines 65-68] "The bit outputs from the plurality of linear shift registers are programmably combined in the non-linear sequence generator according to a first program key.*

to process the added data with a second key.

> *[see col. 2, lines 5-7] "The shuffle position of the bit is programmably controlled in the shuffle register according to a second program key."*

As per claim 2, Richard teaches:

The system according to claim 1, wherein the decryptor is adapted to perform a single pipeline stage decryption.

> *[see col. 4, lines 12-13] "P-Register 9 for generating a maximum length linear pseudo-random bit sequence"*
>
> *[see col.4 lines 15-18] "Four shift registers 12, 14, 16 and 18 are serially connected to comprise the P-Register such that the bit signal present at the last stage of one shift register is used as the input signal for a succeeding stage."*

Examiner is interpreting the linear shift registers taught by Richard as a single processing direction decryption process.

Claims 1-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Luyster, US PGP No. 20010038693.

As per claim 1, Luyster teaches:

A system for protecting data, comprising:

a memory in which encrypted data is stored; and

> *[see paragraph 95] "The data encryption system includes a computing unit for the execution of each round; memory for storing and loading segments."*

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data,

> *[see paragraph 170] "Decryption is the inverse of encryption. In the present invention all the same steps are repeated but in reverse order. Decryption uses ciphertext output as input and recovers the values of the plaintext inputs. Of course, as noted above, what is herein called the decryption operation can be used for encryption, and vice versa."*

the decryptor being adapted to:

variably bit roll the encrypted data,

> *[see paragraph 95] "a bit-moving function capable of rotating bits (or of otherwise moving bits into different positions) of one-to-one round segments by predetermined numbers of bits."*

to fixedly bit shuffle the bit-rolled data,

> *[see paragraph 95] "a linear combination function which provides new round segments using a round operator generally from a first algebraic group to combine two different round segments; and a nonlinear function which affects a round segment based on a value which depends on bits from another round segment, where both round segments are different round segments from the same one-to-one round segment set."*

to add a first key to the bit-shuffled data and

> *[see paragraph 105] "Generally, all embodiments of the system of the present invention have a subkey combining function in each round which provides new round segments by combining a round segment typically linearly with a subkey segment."*

to process the added data with a second key.

> *[see paragraph 154] "After completion of the last round, the system linearly combines (block 82) using the last linear operator of the rounds the left primary round segment R0, with the last subkey value, Klast."*

As per claim 2, Luyster teaches:

The system according to claim 1, wherein the decryptor is adapted to perform a single pipeline stage decryption.

> *[see paragraph 97] "Embodiments of this Feistel or near-Feistel approach generally modify each of the primary round segments in each round of calculation in the same way, typically using operations which modify all the bits of the large primary round segments in single linear operations."*

As per claim 3, Luyster teaches:

The system according to claim 1, wherein the decryptor comprises a bit roller that rotates data in one or more roll regions of the incoming data based on an address related to the received encrypted data and a key related to the first key.

> *[see paragraph 138] "An example of indirect linear combination includes (1) operating on a first variable segment with a fixed rotation and (2) on a second segment by adding to it a predetermined subkey value."*
>
> *[see paragraph 106] "The key expansion method applicable to data-dependent ciphers of the present invention detailed herein provides a rapid subk ey generation method which permits control of the differences between subkeys using fixed table values."*

As per claim 4, Luyster teaches:

The system according to claim 3, wherein the key comprises a shifted version of the first key.

> *[see paragraph 7] "Secret key values are the values which influence the mapping of input to output provided by the block cipher. It is useful to divide secret keys into two categories: secret input keys and secret keys. A secret key is usually of fixed length. A block cipher usually operates on a secret key, but in some cases may operate on an secret input key. If a block cipher first operates on a secret input key, potentially it may use some algorithm to transform the secret input key into a secret key in a standard format. Then, a block cipher expands the secret key to form subkeys whose length or number of bits exceeds that of the secret key.*

As per claim 5, Luyster teaches:

The system according to claim 3, wherein the bit roller comprises a plurality of multiplexers.

> *[see paragraph 125] "Linear Operators are restricted to those operators computed as part of the instruction set of a typical microprocessor which have the properties that (1) given two inputs with an equal probability of containing 0's and 1's, the output of the operator contains generally an equal probability of 0's and 1's, and (2) given that either input is constant, the output is a one-to-one function of the other input."*

As per claim 6, Luyster teaches:

The system according to claim 5, wherein each multiplexer comprises a multiplexer selection input, wherein multiplexer selection bits are input at the multiplexer selection input, and wherein the multiplexer selection bits are generated based on the address related to the received encrypted data and the key related to the first key.

> [see paragraph 125} "More specifically, they are instructions executable on a computing unit having two input segments typically of unsigned integers and one output segment which is typically an unsigned integer, such as addition, xor, addition or subtraction in parallel (such as MMX-style addition of two 64-bit segments, each consisting of 2 values of 32-bits each). A segment is a fixed number of ordered bits, where that number is an integer of at least 2.
>
> [see paragraph 138] "An example of indirect linear combination includes (1) operating on a first variable segment with a fixed rotation and (2) on a second segment by adding to it a predetermined subkey value."

As per claim 7, Luyster teaches:

The system according to claim 1, wherein the decryptor comprises a fixed bit shuffler.

> *[see rejection of claim 1]*

As per claim 8, Luyster teaches:

The system according to claim 7, wherein the fixed bit shuffler comprises a fixed, hard-coded bit shuffler.

> *[see paragraph 124] "In the present example, each block half is computed in one 64-bit register."*

As is commonly known in the art, a register is a special, high-speed storage area within the CPU. All data must be represented in a register before it can be processed and the movement of data in and out of registers can only be manipulated by assembly language programs. Examiner is interpreting the use of a register to process incoming data as teaching a hard-coded bit shuffler.

As per claim 9, Luyster teaches:

The system according to claim 7, wherein the fixed bit shuffler does not add a gate delay to the decryptor.

> *[see paragraph 92] "method for quick key expansion, particularly for encryption rounds with data-dependent rotation, which decreases the time required to prepare a block cipher to encrypt or decrypt digital packets of bytes."*

As per claim 10, Luyster teaches:

The system according to claim 1, wherein the decryptor comprises one or more two-bit adders.

> *[see paragraph 125] "Examples of linear operators include addition, subtraction, SIMD a ddition, SIMD subtraction, and bit-wise exclusive-or, where such SIMD (Single Instruction Multiple Data) operations include either addition or subtraction executed in parallel (e.g., MMX -style addition of 2 segments of 32-bits each from two 64-bit registers).*

As per claim 11, Luyster teaches:

The system according to claim 10, wherein each two-bit adder comprises three exclusive OR (XOR) gates and an AND gate.

> *[see paragraph 355] "To compute the primary round segments R0 and R1 in the first half round, the following procedure is used. First, combine linearly using logic gates (block 384) (such as AND, or and XOR gates) the register R1 with the subkey K2 (block 386) to produce an intermediate segment value."*

As per claim 12, Luyster teaches:

The system according to claim 1, wherein the decryptor comprises an XOR block.

> *[see rejection of claim 11]*

As per claim 13, Luyster teaches:

The system according to claim 12, wherein the XOR block comprises one or more XOR gates.

> *[see rejection of claim 12]*

As per claim 14, Luyster teaches:

The system according to claim 13, wherein each XOR gate comprises a first input and a second input, the first input receiving a bit of the second key, the second input receiving a bit of the added data.

> *[see paragraph 355] "To compute the primary round segments R0 and R1 in the first half round, the following procedure is used. First, combine linearly using logic gates (block 384) (such as AND, or and XOR gates) the register R1 with the subkey K2 (block 386) to produce an intermediate segment value."*

As per claim 15, Luyster teaches:

The system according to claim 1, wherein the first key is a shifted version of a key.

> *[see rejection of claim 3]*

As per claim 16, Luyster teaches:

The system according to claim 15, wherein an amount of shift in the first key is based on an address related to the received encrypted data.

> *[see paragraph 352] "two-step master key expansion process where the encryption used in such key expansion has fixed inputs and has session key values which in general are generated by a linear key expansion process using round-dependent shift operations, and where the variation shown immediately above could be used to compute the encryption used in the key expansion process."*

As per claim 17, Luyster teaches:

The system according to claim 15, wherein the first key is generated substantially in parallel with the decrypting of the encrypted data.

> *[see paragraph 32] "In each round of the block cipher, each register of cipher data is recalculated. This process updates and modifies the initial value of each register, which is the old primary segment, and substitutes a new register value, which is a new primary segment. In this approach, each new primary segment is mapped one-to-one with its old primary segment, all subkey segments and other primary segments being equal."*

Because encrypting and decrypting are done in a single linear process, it is clear that the key has to be generated and be available at the time that the encryption/decryption takes place.

As per claim 18, Luyster teaches:

The system according to claim 1, wherein the decryptor does not add a latency to a processor pipeline.

> *[see paragraph 294] "The s-box cipher method minimizes problems such as pipeline optimization in microprocessor chips and "address generation interlock"."*

As per claim 19, Luyster teaches:

The system according to claim 1, wherein the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor.

> *[see paragraph 227] "Fixed rotations by non-zero numbers of bits are a subset of the possible bit-permutations, and unlike most bit-permutations, have the advantage of generally being executed in one clock cycle on a microprocessor.*

As per claim 20, Luyster teaches:

The system according to claim 1, wherein the decryptor decrypts a word of the encrypted data in a single cycle.

> *[see paragraph 97] "Embodiments of this Feistel or near-Feistel approach generally modify each of the primary round segments in each round of calculation in the same way, typically using operations which modify all the bits of the large primary round segments in single linear operations."*

As per claim 21, Luyster teaches:

The system according to claim 1, wherein the word comprises a 64-bit word.

> *[see rejection of claim 8]*

As per claim 22, Luyster teaches:

The system according to claim 1, wherein the decryptor is adapted to receive encrypted data from the memory.

> *[see rejection of claim 1]*

As per claim 23, Luyster teaches:

A system for protecting data, comprising: a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline.

> *[see rejections of claim 1 and 18]*

As per claim 24, Luyster teaches:

A system for protecting data, comprising: a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor.

[see rejections of claim 1 and 19]

As per claim 25, Luyster teaches:

A system for protecting data, comprising: a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data and decrypts a word of the encrypted data in a single cycle.

[see rejections of claims 1 and 20]

As per claim 26, Luyster teaches:

A system for securing data, comprising: a processor that decrypts encrypted data, the processor being adapted to variably bit roll encrypted data and to fixedly bit shuffle the bit-rolled data.

[see rejection of claim 1]

As per claim 27, Luyster teaches:

The system according to claim 26, wherein the processor is adapted to perform a single pipeline stage decryption.

[see rejections of claim 26 and 2]

As per claim 28, Luyster teaches:

A system according to claim 26, wherein the processor is adapted to add a first key to the bit-shuffled data and to process the added data with a second key.

[see rejection of claim 1]

As per claim 29, Luyster teaches:

The system according to claim 26, wherein the processor is adapted to decrypt the encrypted data without adding a latency to a processor pipeline.

[see rejection of claim 18]

As per claim 30, Luyster teaches:

A method for securing processor instructions, comprising: variably rolling data information based on a first key and an address related to the data information; and hard-coded shuffling of the rolled data information; using one or more keys to process the data information.

[see rejections of claims 1, 3, and 8]

As per claim 31, Luyster teaches:

The method according to claim 30, wherein the rolling, the shuffling and the using are part of a single pipeline stage decryption.

[see rejection of claim 2]

As per claim 32, Luyster teaches:

The method according to claim 30, wherein using one or more keys to process the data information comprises adding the hard-coded data information and a shifted version of the first key.

[see rejections of claim 4 and 8]

As per claim 33, Luyster teaches:

The method according to claim 32, wherein using one or more keys to process the data information comprises processing the added data information with a second key using exclusive OR (XOR) gates.

[see rejection of claim 11]

As per claim 34, Luyster teaches:

The method according to claim 33, wherein the first key is unrelated to the second key.

[see rejection of claim 3, "differences in subkeys…"]

As per claim 35, Luyster teaches:

The method according to claim 30, wherein the data information comprises encrypted data information.

[see rejection of claim 1]

As per claim 36, Luyster teaches:

The method according to claim 30, wherein the encrypted data information is stored in a memory, and wherein the stored data information is accessed by a processor.

[see rejection of claim 1]

As per claim 37, Luyster teaches:

The method according to claim 30, wherein the rolling comprises rotating bits within one or more rolling regions of the data information.

[see rejection of claim 3]

CONCLUSION

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

POINTS OF CONTACT

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang

5/10/07

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/10/07